transmitted at an i-th position is calculated as a function of the coding of the signal and the coding of the respective position in the transmission sequence; and

calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals, the authentication token of the one signal transmitted at the i-th position being a bit-by-bit XOR link or an equivalent logic function of the coding of the one signal and the coding of the respective position in the transmission sequence; and

confirming the transmission sequences by nonintersecting m-bit strings.

REMARKS

Claims 24 to 30 have been added. No new matter has been added. Claims 11 to 30 are pending in the above-identified application.

Applicants respectfully request reconsideration of the present application in view of this response.

Regarding paragraph two (2) of the Office Action, Applicants thank the Examiner for acknowledging the claim for foreign priority for the present application.

Regarding paragraph three (3) of the Office Action, Applicants thank the Examiner for accepting the previously submitted Substitute Specification and withdrawing the 35 U.S.C. § 112 rejections.

Regarding paragraphs four (4) and five (5) of the Office Action, claims 11 to 13, 15, 16, 18, 19, 22 and 23 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,319,710 to Atalla et al. (the "Atalla reference").

The Atalla reference purportedly concerns combining and managing personal verification and message authentication encryptions for network transmission. See Title. The Atalla reference refers to providing a method and means for integrating the encryption keys associated with the personal identification number ("PIN") and message authentication code ("MAC") to assure that the codes are sufficiently interrelated and that alteration of one such code will adversely affect the other such code and inhibit message authentication in the network. See col. 2, lines 10-16. The Atalla reference further refers to the return acknowledgment or non-acknowledgment code being securely returned from node to node in

the network without the need for encryption and decryption at each node, and will still be securely available for proper validation as received at the originating node. See col. 2, lines 16-21. The Atalla reference recites that this is accomplished by using one session key to encrypt the PIN along with the MAC, a random number, the message, and the sequence number which are also encrypted with the PIN such that re-encryption thereof in the transmission from location to location, or node to node over a network is greatly facilitated and validated at each node. See col. 2, lines 21-28. The Atalla reference further refers to portions of the random number being selected for use as the Acknowledgment or Non-Acknowledgment return codes which can be securely returned and which can then only be used once to unambiguously validate the returned code only at the originating node in the network. See col. 2, lines 28-33.

Claim 11 recites a method for transmitting signals between a transmitter and a receiver including:

> calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase; and
>
> calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals.

In contrast, the Atalla reference does not identically disclose (as it must for anticipation) or even suggest at least the feature of calculating an authentication token as a function of the data in the communication phase to authenticate both the signals and transmission sequence of the signal, as in claim 11. In fact, the Atalla reference concerns using one session key to encrypt the PIN along with the MAC, a random number, the message, and the sequence number which are also encrypted with the PIN such that re-encryption thereof in the transmission from location to location. See col. 2, lines 10-28. The Atalla reference further refers to using portions of the random number being selected for use as the Acknowledgment or Non-Acknowledgment return codes which can be securely returned and which can then only be used once to unambiguously validate the returned code only at the originating node in the network. See col. 2, lines 28-33. In claim 11 of the present application, the calculation of an authentication token for the signals is *as a function of the data in the communication phase* so as to authenticate both the signals and the transmission sequence of the signals, as in claim 11. Accordingly, the Atalla reference does not identically

disclose or even suggest the features of claim 11. Withdrawal of the rejection of claim 11 under 35 U.S.C. § 102(b) is respectfully requested.

Since claims 12, 13, 15, 16, 18, 19, 22 and 23 depend from claim 11, those claims are allowable for at least the same reasons as claim 11.

Regarding paragraphs six (6) and seven (7) of the Office Action, claims 14, 17, 20 and 21 were rejected under 35 U.S.C. § 103(a) as unpatentable over the Atalla reference and 'Official Notice.'

Since claims 14, 17, 20 and 21 depend from claim 11, those claims are allowable for at least the same reasons as claim 11, as explained above.

The 'Official Notice,' as apparently applied to claims 20 and 21, refers to assuming that "generation of pseudorandom sequences in this manner are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Atalla. It would have been desirable to do so as the block cipher is well quanified [*sic*] and the output true randomness can accurately be determined."

In view of the above, Applicants submit that the 'Official Notice' in the Office Action does not correct the deficiencies of the Atalla reference. The 'Official Notice' does not disclose the feature of calculating an authentication token as a function of the data in the communication phase to authenticate both the signals and transmission sequence of the signal, as in claim 11.

Further, it is respectfully submitted that the Office Action reflects hindsight, reconstruction and speculation, which caselaw has indicated does not constitute evidence that will support a proper obviousness finding. To the extent that the Office Action recites conclusory and unsupported assertions to wrongly conclude that the 'Official Notice' and Atalla reference disclose or even suggest the features of the claims discussed above, it is respectfully requested pursuant to 37 C.F.R. § 1.104(d)(2) that the Office Action provide an affidavit and/or published information concerning such assertions. In this way, the Applicants may have a fair opportunity to meaningfully and specifically address objective evidence -- as provided for by Rule 104.

As further regard the obviousness rejections, to reject a claim as obvious under 35 U.S.C. § 103, the prior art must disclose or suggest each claim element and it must also

provide a motivation or suggestion for combining the elements in the manner contemplated by the claim. (See Northern Telecom, Inc. v. Datapoint Corp., 908 F.2d 931, 934 (Fed. Cir. 1990), cert. denied, 111 S. Ct. 296 (1990)). The cases of In re Fine, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988), and In re Jones, 21 U.S.P.Q.2d 1941 (Fed. Cir. 1992), also make plain that the Office Action's assertions that it would have been obvious to modify the reference relied upon does not properly support a 35 U.S.C. § 103 rejection. It is respectfully suggested that those cases make plain that the Office Action reflects a subjective "obvious to try" standard, and therefore does not reflect the proper evidence to support an obviousness rejection based on the references relied upon.

Thus, as discussed above, the Atalla reference and 'Official Notice,' alone or in combination, do not describe or suggest the claimed features. Withdrawal of the rejection of claims 14, 17, 20 and 21 under 35 U.S.C. §103(a) over the Atalla reference and 'Official Notice' is respectfully requested.

New claims 24 to 30 contain analogous features to claims 11 to 23; accordingly, it is respectfully submitted that those claims are also allowable over the art cited in the Office Action for essentially the same reasons as for claims 11 to 23. No new matter has been added.

In summary, it is respectfully submitted that all of claims 11 to 30 of the present application are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that the rejections of claims 11 to 23 have been obviated. Accordingly, it is respectfully submitted that all claims 11 to 30 are allowable.

It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

If it would further allowance of the present application, the Examiner is warmly invited to contact the undersigned.

Respectfully submitted,

By: Jud Sanders
Reg. No. 47084

Dated: June 27, 2003

By: Richard L. Mayer
Richard L. Mayer
(Reg. No. 22,490)

CUSTOMER NO. 26646

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200